Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. (Previously Presented) A method of addressing data errors in a computer system, comprising:

error-checking a unit of data;

if at least one uncorrectable error is detected in the unit of data, determining if the at least one uncorrectable error is a data poisoning event, and if so, marking the unit of data with an indication that the unit of data contains a data poisoning event;

determining, based on a data poisoning policy, if the data poisoning event is to be acted upon, and if so, detecting, by the computer system, the presence of the indication that the unit of data contains a data poisoning event; and

acting, by an operating system of the computer system, upon the presence of the indication to address the presence of erroneous data in the unit of data, wherein the operating system is not always brought down upon the presence of the indication.

2. (Original) The method of Claim 1, wherein said error-checking comprises:

applying error-control decoding to the unit of data.

3. (Original) The method of Claim 2, wherein said error-checking further comprises:

correcting any correctable errors in the unit of data.

4. (Cancelled)

5. (Original) The method of Claim 1, wherein said acting upon the presence of the indication

comprises:

removing the unit of data from use by the operating system.

6. (Original) The method of Claim 5, wherein said acting upon the presence of the indication further comprises:

recovering the unit of data.

7. (Cancelled)

8. (Previously Presented) The method of Claim 1, further comprising:

if the operating system detects the presence of said indication that the unit of data contains a data poisoning event, determining if the unit of data is in user space; and

if the unit of data is in user space, terminating an application running on the computer system and removing the unit of data from use by the operating system.

9. (Original) The method of Claim 1, further comprising:

upon detection of an uncorrectable error in said unit of data, providing information to said operating system to enable recovery of said unit of data.

10. (Original) The method of Claim 9, wherein the information includes a target address corresponding to said unit of data.

11. (Original) The method of Claim 1, further comprising:

determining whether or not to take immediate action on detection of a data-poisoning error.

12. (Original) The method of Claim 11, wherein said determining whether or not to take immediate action on detection of a data-poisoning error comprises:

setting a software-visible control bit.

13. (Previously Presented) The method of Claim 1, wherein said detecting is performed by at least one unit selected from the group consisting of: a processor and a memory.

14. (Previously Presented) A computer system comprising:

at least one processor;

at least one error control decoding implementation selected from the group consisting of an error-control decoder, software to implement error-control decoding by the at least one processor, and firmware to implement error-control decoding in conjunction with the at least one processor, adapted to process units of data and to determine if a unit of data contains at least one uncorrectable error;

a module to run on said at least one processor to determine if said at least one uncorrectable error is a data poisoning event and, if so, to mark as containing a data poisoning event a unit of data containing said at least one uncorrectable error; and

at least one operating system to run on said at least one processor, the operating system to implement a policy to determine if a particular data poisoning event is to be acted upon or not, the operating system adapted to detect the presence of a unit of data marked as containing a data poisoning event, if the data poisoning event is to be acted upon, and to act upon said presence to mitigate the at least one uncorrectable error without always bringing down the operating system upon detection of a unit of data marked as being bad.

15. (Previously Presented) The computer system of Claim 14, further comprising:

a memory coupled to said at least one error control decoding implementation selected from the group consisting of an error-control decoder, software to implement error-control decoding, and firmware to implement error-control decoding, wherein the at least one error-control decoding implementation is adapted to process units of data stored in the memory.

16. (Original) The computer system of Claim 14, wherein said memory comprises:

a processor cache.

17. (Original) The computer system of Claim 14, further comprising:

at least one bus coupled to said at least one of an error-control decoder, software to implement error-control decoding, and firmware to implement error-control decoding, wherein the at least one of an error-control decoder, software to implement error-control decoding, and firmware to implement error-control decoding is adapted to process units of data passing through the at least one bus.

18. (Original) The computer system of Claim 14, further comprising:

logic adapted to control signaling of information relating to one or more uncorrectable data errors.

19. (Original) The computer system of Claim 18, wherein the logic comprises:

programmable logic.

20. (Original) The computer system of Claim 18, wherein the information includes a target address corresponding to a unit of data containing at least one uncorrectable error.

21. (Currently Amended) A ~~tangible~~ physical machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

error-checking a unit of data;

if at least one uncorrectable error is detected in the unit of data, determining if the at least one uncorrectable error is a data poisoning event, and if so, marking the unit of data with an indication that the unit of data contains a data poisoning event;

determining, based on a data poisoning policy, if the data poisoning event is to be acted upon, and if so, detecting, by the computer system, the presence of the indication that the unit of data

contains a data poisoning event; and

acting, by an operating system of the computer, upon the presence of the indication to address the presence of erroneous data in the unit of data, wherein the operating system is not always brought down upon the presence of the indication.

22. (Currently Amended) The physical machine-accessible medium of Claim 21, further comprising software code that, when read by a computer, causes the computer to also perform the following:

if the operating system detects the presence of said indication that the unit of data contains a data poisoning event, determining if the unit of data is in user space; and

if the unit of data is in user space, terminating an application running on the computer and removing the unit of data from use by the operating system.

23. (Currently Amended) The physical machine-accessible medium of Claim 21, wherein said acting upon the presence of the indication comprises:

removing the unit of data from use by the operating system.

24. (Currently Amended) A computer system comprising:

at least one processor; and

at least one ~~tangible~~ physical machine-accessible medium to be coupled to the at least one processor, the at least one processor to access the at least one physical machine-accessible medium and to execute software code stored on the at least one physical machine-accessible medium, to cause the computer system to perform a method comprising:

error-checking a unit of data;

if at least one uncorrectable error is detected in the unit of data, determining if the at least one uncorrectable error is a data poisoning event, and if so, marking the unit of data with an indication that the unit of data contains a data poisoning event;

determining, based on a data poisoning policy, if the data poisoning event is to be acted upon,

and if so, detecting the presence of the indication that the unit of data contains a data poisoning event; and

acting, by an operating system of the computer system, upon the presence of the indication to address the presence of erroneous data in the unit of data, wherein the operating system is not always brought down upon the presence of the indication.

25. (Currently Amended) The computer system of Claim 24, wherein the at least one physical machine-accessible medium further comprises software code that, when executed by the at least one processor, causes the computer system to further performs:

if the operating system detects the presence of said indication that the unit of data contains a data poisoning event, determining if the unit of data is in user space; and

if the unit of data is in user space, terminating an application running on the computer and removing the unit of data from use by the operating system.

26. (Currently Amended) The computer system of Claim 24, wherein the at least one physical machine-accessible medium further comprises software code that, when executed by the at least one processor, causes the computer system to further performs:

removing the unit of data from use by the operating system.

27. (Currently Amended) The computer system of Claim 24, further comprising:

at least one bus coupling the at least one processor with the at least one physical machine-accessible medium.